CLAIMS

What is Claimed is:

1. A method comprising:

comparing outbound traffic on a host computer system to inbound traffic on the host computer system; and

determining if malicious code is detected on the host computer system based on the comparing.

2. The method of Claim 1, further comprising:

if malicious code is detected, providing a notification of the malicious code detection.

3. The method of Claim 1, wherein the comparing is performed using a similarity comparison technique.

4. The method of Claim 1, wherein at least a portion of the outbound traffic is compared to at least a recently received portion of the inbound traffic, the at least a portion of the outbound traffic being subsequent in time to the at least a recently received portion of the inbound traffic.

5. The method of Claim 1, wherein the inbound traffic is received at the host computer system from a source port,

and wherein the outbound traffic is for sending to a destination port,

and further wherein the source port and the destination port are the same port.

6. The method of Claim 1, wherein the inbound traffic is received on the host computer system from a source port,

and wherein the outbound traffic is for sending to an destination port,

and further wherein the source port and the destination port are different ports.

7. The method of Claim 2, further comprising:

implementing protective actions.

8. The method of Claim 2, further comprising:

intercepting the inbound traffic;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting the outbound traffic;

copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic; and

releasing the outbound traffic.

9. The method of Claim 8, wherein the comparing comprises:

comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

10. The method of Claim 2, further comprising:

intercepting the inbound traffic;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting the outbound traffic;

buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic; and

if malicious code is not detected releasing the buffered outbound traffic.

11. The method of Claim 10, wherein the comparing comprises:

comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic.

12. A malicious code detection device comprising:

an interception function;

at least one inbound traffic memory area coupled to the interception function;

at least one outbound traffic memory area coupled to the interception function; and

a comparator coupled to the at least one inbound traffic memory area and the at least one outbound traffic memory area.

13. The malicious code detection device of Claim 12, further comprising:

a prior name resolution correlation function.

14. The malicious code detection device of Claim 13, wherein the prior name resolution correlation function is included in the interception function.

15. A method comprising:

intercepting inbound traffic on a host computer system;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting outbound traffic on the host computer;

copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic;

releasing the outbound traffic;

comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic;

determining if malicious code is detected on the host computer system based on the comparing; and

if malicious code is detected, providing a notification of the malicious code detection.

16. The method of Claim 15, wherein the comparing is performed using a similarity comparison technique.

17. The method of Claim 15, wherein the at least a portion of the copied outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic.

18. The method of Claim 15, further comprising:

prior to the copying the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic.

19. The method of Claim 15, wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis,

and wherein the outbound traffic is copied to the outbound traffic memory area on a per destination port basis.

20. A method comprising:

intercepting inbound traffic on a host computer system;

copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic;

releasing the inbound traffic;

intercepting outbound traffic on the host computer;

buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic;

comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic;

determining if malicious code is detected on the host computer system based on the comparing;

if malicious code is detected, providing a notification of the malicious code detection; and

if malicious code is not detected, releasing the at least a portion of the buffered outbound traffic.

21. The method of Claim 20, wherein the comparing is performed using a similarity comparison technique.

22. The method of Claim 20, wherein the at least a portion of the buffered outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic.

23. The method of Claim 20, further comprising:

prior to buffering the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic.

24. The method of Claim 20, wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis,

and wherein the outbound traffic is buffered in the outbound traffic memory area on a per destination port basis.